R. W. Spekkens[1]* and T. Rudolph[2]†

[1] *Department of Physics, University of Toronto, 60 St. George Street, Toronto, Ontario, Canada, M5S 1A7*

[2] *Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Vienna, Austria*

(July 9, 2001)

The Mayers-Lo-Chau theorem establishes that no quantum bit commitment protocol is unconditionally secure. Nonetheless, there can be non-trivial upper bounds on both Bob's probability of correctly estimating Alice's commitment and Alice's probability of successfully unveiling whatever bit she desires. In this paper, we seek to determine these bounds for generalizations of the BB84 bit commitment protocol. In such protocols, an honest Alice commits to a bit by randomly choosing a state from a specified set and submitting this to Bob, and later unveils the bit to Bob by announcing the chosen state, at which point Bob measures the projector onto the state. Bob's optimal cheating strategy can be easily deduced from well-known results in the theory of quantum state estimation. We show how to understand Alice's most general cheating strategy, (which involves her submitting to Bob one half of an entangled state) in terms of a well known theorem of Hughston, Josza and Wootters. We also show how the problem of optimizing Alice's cheating strategy for a fixed submitted state can be mapped onto a problem of state estimation. Finally, using the Bloch ball representation of qubit states, we identify the optimal coherent attack for a class of protocols that can be implemented with just a single qubit. These results provide a tight upper bound on Alice's probability of successfully unveiling whatever bit she desires in the protocol proposed by Aharonov *et al.*, and lead us to identify a qubit protocol with an even stronger bound.

I. INTRODUCTION

Suppose Alice and Bob wish to play a game wherein Alice wins if she can correctly predict which of two mutually exclusive events will occur and Bob wins if she cannot. One way to play the game would be for Alice to tell Bob her prediction before the events in question. There are situations, however, where this is inappropriate. For instance, Bob might be able to influence the relative probability of the events in question (indeed, which of these events occurs might be entirely up to Bob). In such cases, Alice wants Bob to know as little as possible about her prediction until some time after the occurrence of one of these events being predicted. Of course, Bob will still want to receive some sort of 'token' of Alice's prediction prior to the events in question, since otherwise Alice could always claim to have won the game. Thus, Alice and Bob would like a cryptographic protocol which forces Alice to 'commit' herself to a bit (which encodes her prediction), while ensuring that Bob can find out as little as possible about this bit until the time that Alice reveals it to him. This is a bit commitment(BC) protocol. In addition to the task of prediction described above, BC appears as a primitive in many other cryptographic tasks and is therefore of particular significance in cryptography.

A simple example of an implementation of BC proceeds as follows. Alice writes a '0' or a '1' on a piece of paper, and locks this in a safe. She then sends the safe to Bob, but keeps the key. When it comes time to reveal her commitment, she sends the key to Bob, who opens the safe and discovers the value of the bit. This protocol binds Alice to the bit she chose at the outset since she cannot change what is written on the piece of paper after she submits the safe to Bob. However, it only conceals the bit from Bob if he is unable to pick the lock, or force the safe open, or image the contents of the safe.

This paper focuses on a particular class of quantum BC protocols, specifically, generalizations of the BC protocol proposed by Bennett and Brassard in 1984 [1]. We shall refer to these as *generalized BB84 BC protocols*. Within such protocols, an honest Alice commits to a bit 0 by choosing a state randomly from a specified set of states, and by subsequently sending a system prepared in this state to Bob. She commits to a bit 1 by choosing the state from a different set. At the end of the protocol she reveals to Bob which state she submitted and Bob measures the projector onto this state to verify Alice's claim.

Bob can cheat in such a protocol by performing a measurement on the systems submitted to him by Alice, prior to Alice revealing her commitment. The measurement that maximizes his probability of correctly estimating Alice's commitment can be determined from the well-known

*spekkens@physics.utoronto.ca †terry@ap.univie.ac.at

theory of state estimation [2] [3].

Alice can cheat by preparing the system she initially submits to Bob in a state different from the ones specified by the protocol, in particular, by entangling this system with an ancilla system that she keeps in her possession, and by later performing a measurement on the ancilla and choosing the state which she announces to Bob based on the outcome of this measurement. This has been called a *coherent attack*, since in general such an attack requires Alice to maintain the coherence between the different possibilities in the random choice the protocol asks her to make. It has also been called an *EPR-type attack*, since in the original BB84 BC protocol, the optimal entangled state for Alice to prepare is the EPR state. The problem of determining the coherent attack that maximizes Alice's probability of successfully cheating has remained open to date. It is the goal of this paper to begin to answer this question.

It has been shown by Mayers [4] and by Lo and Chau [5] that an unconditionally secure BC protocol does not exist [6]. In other words, it is not possible to devise a BC protocol that is *arbitrarily concealing*, *i.e.* one for which Bob's probability of correctly estimating Alice's commitment is arbitrarily small, and *arbitrarily binding*, *i.e.* one for which Alice's probability of revealing whatever bit she desires without being caught cheating is arbitrarily small. Nonetheless, there remain interesting questions to be answered about coherent attacks. For instance, it *is* possible to have a BC protocol that is *partially binding* and *partially concealing*, wherein Alice and Bob's probabilities of successfully cheating are both bounded above [7]. Determining the optimal coherent attack is crucial to determining the degree of bindingness that can be achieved in such protocols.

Coherent attacks are also important in other quantum cryptographic tasks between mistrustful parties - such as coin tossing [8], cheat sensitive bit commitment [9], bit escrow [10] and quantum gambling [11] - wherein a type of bit commitment often appears as a subprotocol. Understanding how to optimize coherent attacks is therefore important for settling questions about the degree of security that can be achieved for such tasks.

We summarize here the main results of the paper. The last four apply only to protocols that can be implemented using a single qubit.

- We explain coherent attacks in terms of the well-known theorem of Hughston, Josza and Wootters [12].
- We demonstrate that the problem of finding the optimal coherent attack for a *fixed* submitted state can be mapped onto a problem of state estimation.
- We show that the optimal state for a cheating Alice to submit has a support in the span of the supports of the states which an honest Alice chooses from.
- We provide a simple geometrical picture on the Bloch sphere of coherent attacks. In addition to being useful for building one's intuitions about such attacks, this provides a convenient formalism within which to solve the optimization problem, as well as a geometrical criterion for whether or not Alice can cheat with probability 1 in a given protocol.
- We find analytic expressions for the optimal cheating strategy in the case where the sets of states that an honest Alice chooses from each have no more than two elements.
- Using these results, we determine Alice's optimal coherent attack in a BC protocol that was proposed by Aharonov *et al.* [10]. Our result provides a tight upper bound on Alice's probability of unveiling whatever bit she desires, improving upon the best previous known upper bound. This allows us to determine, for this protocol, the trade-off relation between the degree of concealment and the degree of bindingness. We show that the same trade-off relation can be achieved with several other protocols.
- Finally, our results allow us to determine Alice's optimal coherent attack in a new type of generalized BB84 BC protocol wherein the trade-off relation between concealment and bindingness is better than can be achieved with the protocol of Aharonov *et al.*

The paper is organized as follows. In section II, we provide an operational definition of bit commitment, define degrees of security, and describe the BB84 BC protocol and its generalization. In section III, we introduce the notion of a convex decomposition of a density operator, review its properties, and demonstrate its significance for coherent attacks. In section IV, we formulate the optimization problem to be solved. Results for protocols involving systems of arbitrary dimensionality and for protocols involving qubits are presented in sections V and VI respectively. Applications of these results are presented in section VII, and section VIII contains our concluding remarks.

II. BIT COMMITMENT

A. An operational definition of Bit Commitment

We begin by providing a definition of BC that is strictly operational, that is, one which only makes reference to the experimental operations carried out by the parties, and not to any concepts that are particular to a physical theory. This seems to us to be the most sensible way of proceeding for *any* information processing task, since such tasks can be defined independently of their physical implementation and consequently of any physical theory describing this implementation. Among other benefits, this approach allows one to characterize a physical theory by the type of protocols which can be securely implemented within a universe described by that theory.

A BC protocol is a cryptographic protocol between two mistrustful parties. It can be defined in terms of the characteristics of these parties' honest (*i.e.*, non-cheating) strategies. We call the two parties Alice and Bob, and assume that Alice is the one making the commitment.

The protocol is divided into three intervals, called the commitment phase, the holding phase and the unveiling phase. Each of these may involve many rounds of communication between Alice and Bob. The result of the protocol is one of three possibilities, denoted '0', '1' and 'fail'. Which of these has occurred is determined from the outcomes of all the measurements that an honest Bob has made throughout the protocol. The protocol specifies the strategy an honest Alice must adopt to commit to a bit b. It is such that if both parties are honest and Alice follows the strategy for committing a bit 0(1), the result of the protocol is necessarily '0'('1'). It follows that if the outcome 'fail' occurs, an honest Bob can conclude that Alice must have cheated. The protocol must also be such that if both parties are honest, Alice does not, through actions taken after the end of the commitment phase, change the relative probability of the results '0' and '1' occurring, and Bob does not, prior to the beginning of the unveiling phase, gain any information about Alice's commitment.

In the protocols we shall be considering, Alice will not always be caught when she cheats. Thus, it can happen that the result of the protocol is 'b' even though Alice cheated and did not follow the honest strategy for committing a bit b. Indeed, Alice can, by cheating, change the relative probability of the '0' and '1' results by actions taken after the commitment phase. Since Alice can influence the result of the protocol by her choice of cheating strategy, we shall say that 'Alice unveils bit b' whenever the result 'b' occurs.[1]

B. Types of security

To define the security of a BC protocol, one needs to quantify the notions of concealment against Bob and bindingness against Alice. In this paper, we focus upon the probability that Bob can, prior to the beginning of the unveiling phase, correctly estimate Alice's commitment (given that Alice is honest), and the probability that Alice can, after the end of the commitment phase, successfully unveil whatever bit she desires (given that Bob is honest). We denote these by P_E and P_U respectively. Note that these probabilities vary with the cheating strategy used. In this paper, we shall only consider protocols wherein these are both equal to 1/2 for honest strategies.[2]

A bit commitment protocol is said to be *arbitrarily binding* if for all of Alice's strategies, P_U is bounded above by $1/2 + \varepsilon$, where ε can be made arbitrarily small by increasing some security parameter in the protocol. It is said to be *arbitrarily concealing* if for all of Bob's strategies, P_E is bounded similarly. Although, as we shall discuss shortly, no BC protocol can be arbitrarily binding and arbitrarily concealing, both P_E and P_U *can* have non-trivial upper bounds (that is, upper bounds less than 1). We will refer to such protocols as *partially binding* and *partially concealing.* The maxima of P_E and P_U for a given protocol, which we denote by $P_E^{\max}$ and $P_U^{\max}$, quantify the degree of concealment and the degree of bindingness that can be achieved in this protocol.

The implementation of BC using a safe, discussed in the introduction, is binding against Alice, but is only concealing against Bob if he has limited 'safe-cracking' resources. More useful implementations of bit commitment instead rely for concealment on the assumption that Bob has limited computational resources. Obviously, one would prefer that the security of the protocol not depend on the resources of either party, but rather only on the laws of physics and the integrity of the party's laboratories. A property of a protocol that has this feature is said to hold *unconditionally.* All the properties of protocols referred to in this paper, are properties which hold unconditionally.

[1] It is important to remember that within our terminology 'Alice unveiling bit b' implies that she was not caught cheating. Thus in a generalized BB84 BC protocol, when Alice announces b to Bob, we say that Alice is *attempting* to unveil a bit b, but we only say that she has unveiled b if she passes Bob's test.

[2] In most discussions of bit commitment, it is assumed that neither Alice nor Bob has any information at the commitment phase about which bit will be more beneficial for Alice to unveil. However, one must relax this assumption in order to consider a game wherein Alice predicts which of two events will occur given some prior information on their relative probability. The results of this paper can be generalized in a straightforward manner to apply to such a protocol. It suffices to replace Eq. (5) with $P_U = p_0 P_{U0} + p_1 P_{U1}$, where p_b is the probability that Alice will wish to unveil bit b after the commitment phase, and to generalize all subsequent expressions accordingly.

C. The BB84 BC protocol

The first proposal for a quantum mechanical implementation of a BC protocol was made by Bennett and Brassard [1]. We refer to it as the BB84 BC protocol. This was recognized by its authors to have no bindingness against Alice. Nonetheless, we begin by reviewing this protocol, since it provides a simple example of the type of cheating strategy with which this paper will be concerned.

Imagine a protocol wherein Alice submits a qubit to Bob during the commitment phase. To commit to a bit 0, she prepares the qubit in a state chosen uniformly from the set $\{|0\rangle, |1\rangle\}$, while to commit to a bit 1, she chooses from the set $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. No measurement Bob can do is able to distinguish these two possibilities. At the unveiling phase, Alice can tell Bob which state she submitted, and Bob can do a measurement of the projector onto this state to verify her honesty. If Alice tries to convince Bob that she submitted a state drawn from the opposite set - for instance, that she submitted $|+\rangle$ when in fact she submitted $|0\rangle$ - then her probability of passing his test is only 1/2. The BB84 BC protocol demands that Alice repeat her commitment for N qubits, that is, that Alice either chooses each qubit's state uniformly from $\{|0\rangle, |1\rangle\}$ or uniformly from $\{|+\rangle, |-\rangle\}$. Clearly, in this case her probability of passing Bob's test when she lies about her commitment is $1/2^N$. So, with respect to strategies wherein Alice cheats by lying about her commitment, such a protocol appears to be arbitrarily binding.

However, Alice has another cheating strategy available to her. Prior to submitting a qubit to Bob, she can entangle it with a qubit that she keeps in her possession. Specifically, she prepares the two in the EPR state $(|0\rangle|1\rangle - |1\rangle|0\rangle)/\sqrt{2}$. Given that this state can also be written as $(|+\rangle|-\rangle - |-\rangle|+\rangle)/\sqrt{2}$, it is clear that by measuring the $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$ basis on the qubit in her possession, she projects the qubit in Bob's possession into the $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$ basis respectively. Moreover, the binary outcome of her measurement will be perfectly anti-correlated with the state of Bob's qubit. So Alice knows precisely which state to announce to Bob. Using this strategy, she can choose which bit she wants to unveil just prior to the unveiling phase, and always succeed at passing Bob's test. This is the so-called 'coherent' or 'EPR' attack.

The analysis thus far leaves open the possibility that some other protocol using quantum primitives might succeed where the BB84 protocol failed. In fact, it has been shown that for the most general nonrelativistic protocol, unconditional security is not possible [4] [5] [8]. Nonetheless, there exist simple generalizations of the BB84 protocol that are both partially concealing and partially binding.

D. Generalizations of the BB84 BC protocol

A generalized BB84 BC protocol defines two sets of states $\{\psi_k^0\}_{k=1}^{n_0}$ and $\{\psi_k^1\}_{k=1}^{n_1}$ and corresponding probability distributions $\{p_k^0\}_{k=1}^{n_0}$ and $\{p_k^1\}_{k=1}^{n_1}$ (note that the values of n_0 and n_1 may not be the same). In order to commit to bit b, an honest Alice chooses a state from $\{\psi_k^b\}_{k=1}^{n_b}$ using the distribution $\{p_k^b\}_{k=1}^{n_b}$ and sends a system prepared in this state to Bob at the commitment phase. An honest Bob simply stores the system during the holding phase. At the unveiling phase, an honest Alice announces b and k to Bob, and he measures the projector onto $|\psi_k^b\rangle$. If Alice passes Bob's test, she has succeeded in unveiling the bit b, and the result of the protocol is 'b'. Otherwise, she is caught cheating, and the result of the protocol is 'fail'.[3]

To estimate Alice's commitment, Bob must estimate whether the system in his possession is described by $\rho_0 = \sum_{k=1}^{n_0} p_k^0 |\psi_k^0\rangle\langle\psi_k^0|$, or $\rho_1 = \sum_{k=1}^{n_1} p_k^1 |\psi_k^1\rangle\langle\psi_k^1|$. The problem of optimal state estimation has previously been studied in great detail [2] [3], and in particular the optimal measurement for discriminating two density operators is well known. Using the optimal measurement, the maximum probability of Bob correctly estimating Alice's commitment is

$$P_E^{\max} = \frac{1}{2} + \frac{1}{4}\mathrm{Tr}\,|\rho_0 - \rho_1|, \tag{1}$$

where $|A| = \sqrt{A^\dagger A}$. It follows that as long as ρ_0 and ρ_1 do not have orthogonal supports, $P_E^{\max}$ is strictly less than 1 and the protocol is partially concealing.

The complementary problem, of determining the maximum probability of Alice unveiling whatever bit she desires and the strategy which achieves this maximum, has remained open to date. Alice's most general strategy is of the following form. Prior to sending the system to Bob, she entangles it with a system she keeps in her possession. At the unveiling phase, she does one of two measurements on the system in her possession, depending on whether she is attempting to unveil a 0 or a 1. She chooses what integer k to announce to Bob based on the

---

[3] It should be noted that the honest strategy for Alice to commit b that we have described is equivalent with respect to concealment to the following strategy: Alice couples the system she sends to Bob with a system she keeps in her possession (of dimension n_b or greater) such that the two are in the entangled state $\sum_{k=1}^{n_b} \sqrt{p_k^b}\, |k\rangle \otimes |\psi_k^b\rangle$, where the $|k\rangle$ form an orthonormal basis. At the unveiling phase, she measures the basis $|k\rangle$ in order to determine what integer to announce to Bob.

outcome of this measurement. It follows that in order to determine $P_U^{\max}$, we must optimize over the entangled state that Alice prepares, the two measurements she can perform and the announcement she makes to Bob given each possible outcome.

We shall see that there exist generalized BB84 BC protocols where $P_U^{\max}$ is strictly less than 1, so that these protocols are partially binding.

It will be useful to introduce a few mathematical concepts and results before turning to the optimization problem.

III. CONVEX DECOMPOSITIONS OF A DENSITY OPERATOR

A. Definition and properties of convex decompositions

We begin by introducing a mathematical concept that will be critical for solving our problem. A *convex decomposition* $\{(q_k, \sigma_k)\}_{k=1}^{n}$ of a density operator ρ is a set of probabilities, q_k, and distinct density operators, σ_k, such that

$$\rho = \sum_{k=1}^{n} q_k \sigma_k .$$

The σ_k will be referred to as the *elements* of the convex decomposition. We use the term 'convex' to distinguish this from a decomposition of a pure state into a sum of pure states, and from a decomposition of a density operator into general sums of operators, that is, sums of operators that are not necessarily positive. Nonetheless, we will throughout this paper use the term *decomposition* as a shorthand.[4]

Some terminology will be used in connection with convex decompositions. The elements that receive non-zero probability will be called the *positively-weighted* elements. A decomposition will be called *extremal* if its positively-weighted elements are all of rank 1 (i.e. if they are all pure states). A set of density operators will be called *uncontractable* if none of its members can be written as a convex decomposition of the others. A convex decomposition will be called uncontractable if its positively-weighted elements are uncontractable. Clearly, all extremal decompositions are uncontractable. Finally, a decomposition of ρ is *trivial* if its only positively-weighted element is ρ.

Another concept that will be useful in the present investigation is a relation that holds between sets of density operators, and which we shall refer to as *composable coincidence.* Two sets of density operators $\{\sigma_k^0\}$ and $\{\sigma_k^1\}$ will be called composably coincident if there exist probability distributions $\{q_k^0\}$ and $\{q_k^1\}$ such that

$$\sum_k q_k^0 \sigma_k^0 = \sum_k q_k^1 \sigma_k^1 .$$

In other words, $\{\sigma_k^0\}$ and $\{\sigma_k^1\}$ are composably coincident if there exists a density operator which has a convex decomposition in terms of the σ_k^0's and a convex decomposition in terms of the σ_k^1's.

It will also be useful to set forth a few well-known facts about convex decompositions [12]. A necessary and sufficient condition for a density operator σ to appear in some convex decomposition of ρ is for the eigenvectors of σ to be confined to the support of ρ. The cardinality of an extremal decomposition of ρ must be greater than or equal to the rank of ρ. Finally, there sometimes exists a prescription for obtaining the probability with which a particular element appears in a convex decomposition of a density operator. In convex decompositions of ρ containing *orthogonal* elements, the probability associated with an element σ is fixed by ρ and σ - it is simply $\mathrm{Tr}(\sigma\rho)/\mathrm{Tr}\left(\sigma^2\right)$. However, for a general set of non-orthogonal elements $\{\sigma_k\}$ that form a convex decomposition of ρ, the probabilities need not be unique; the same set of density operators $\{\sigma_k\}$ may appear in different convex decompositions of ρ. For instance, the completely mixed state in a 2d Hilbert space, $I/2$, has an indenumerably infinite number of convex decompositions with elements $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|\}$, since these yield a decomposition for every probability distribution of the form $\left(\frac{1}{2}\lambda, \frac{1}{2}\lambda, \frac{1}{2}(1-\lambda), \frac{1}{2}(1-\lambda)\right)$ where λ is between 0 and 1. Nonetheless, a special case wherein the probabilities *are* unique is if the convex decomposition is extremal and of cardinality equal to the rank of ρ. In this case, a simple formula for the probability of a given element can be given. If $\{(q_k, |\xi_k\rangle\langle\xi_k|)\}$ is such a decomposition, then the non-zero probabilities are given by Jaynes' rule [13],

$$q_k = \frac{1}{\langle\xi_k|\,\rho^{-1}\,|\xi_k\rangle}, \tag{2}$$

where ρ^{-1} is the inverse of the restriction of ρ to its support.

B. The connection between convex decompositions and POVMs

The most general measurement on a system in quantum mechanics is associated with a *positive operator valued measure(POVM).* A POVM is a set of positive operators that sum to the identity operator, that is, a

[4]Note that previous authors have used the term ρ*-ensemble* to refer to a convex decomposition of ρ.

set $\{E_k\}$ such that for every k, $\langle\phi| E_k |\phi\rangle \geq 0$ for all $|\phi\rangle \in \mathcal{H}$, and $\sum_k E_k = I$. Neumark's theorem [14] shows that every POVM on a system can be implemented by coupling to an ancilla system and performing projective measurements on the ancilla. As it turns out, there is a close mathematical connection between convex decompositions of ρ and POVMs, as was demonstrated by Hughston, Josza and Wootters [12].

Lemma There is a one-to-one map between the convex decompositions of ρ and the POVMs over the support of ρ. Specifically, the POVM $\{E_k\}_{k=1}^n$ is associated with the decomposition $\{(q_k, \sigma_k)\}_{k=1}^n$ defined by

$$q_k \sigma_k = \sqrt{\rho} E_k \sqrt{\rho}. \tag{3}$$

Proof. It is trivial to see that $\{(q_k, \sigma_k)\}_{k=1}^n$ is a decomposition of ρ by summing the above equation over k and using the fact that $\sum_k E_k = I$. That *any* decomposition of ρ is associated with *some* POVM follows from the fact that $\sqrt{\rho}$ is invertible on the support of ρ. Specifically, if this inverse is denoted by $\rho^{-1/2}$ then the resolution $\{(q_k, \sigma_k)\}_{k=1}^n$ is associated with the POVM $\{E_k\}_{k=1}^n$ defined by $E_k = q_k \rho^{-1/2} \sigma_k \rho^{-1/2}$. $\square$.

We will also say that the POVM $\{E_k\}_{k=1}^n$ *generates* the convex decomposition $\{(q_k, \sigma_k)\}_{k=1}^n$. Note that we do not treat the technicalities associated with decompositions of infinite cardinality in this paper, however a discussion of these can be found in Cassinelli *et al.* [15].

C. The significance of convex decompositions to coherent attacks

Suppose Alice and Bob share an entangled state for which ρ is the reduced operator on Bob's system. Prior to any measurements, the best Alice can do in predicting the outcomes of Bob's measurements is to use the density operator ρ in the Born rule. However, by virtue of the correlations between her system and Bob's, if she performs a measurement and takes note of the outcome, her ability to predict the outcomes of Bob's measurements will increase. Since all of the information that is relevant to Alice predicting the outcomes of Bob's measurements is encoded in a density operator, it follows that when she learns the outcome of her measurement, she should update the density operator with which she describes Bob's system. Suppose that the kth outcome occurs with relative frequency q_k, and leads Alice to update the density operator with which she describes Bob's system to σ_k. We say that the statistics of possible updates of Alice's description of Bob's system are given by $\{(q_k, \sigma_k)\}$, that is, a set of probabilities and density operators.

As it turns out, the possibilities for these statistics are given by the convex decompositions of ρ. Specifically, we have:

HJW Theorem For *every* measurement Alice can do, the statistics of possible updates of her description is given by *some* convex decomposition of ρ, and for *every* convex decomposition of ρ, there exists *some* measurement for which the statistics of possible updates is given by that decomposition.

This was first demonstrated for extremal convex decompositions by Hughston, Josza and Wootters [12], and it is straightforward to generalize the proof to arbitrary convex decompositions. Since this theorem is the key to coherent attacks, we present the proof here.

Proof. Suppose Alice and Bob share a state $|\psi\rangle$ that is any purification of ρ (a purification of ρ is any normalized vector $|\Phi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\mathrm{Tr}_A (|\Phi\rangle\langle\Phi|) = \rho$). If the non-zero eigenvalues of ρ are denoted by λ_j, and $\{|e_j\rangle\}$ is a set of normalized eigenvectors associated with these eigenvalues, then $|\psi\rangle$ can always be written as

$$|\psi\rangle = \sum_j \sqrt{\lambda_j} |f_j\rangle \otimes |e_j\rangle,$$

where $\{|f_j\rangle\}$ is a set of orthonormal vectors for Alice's system. This way of writing $|\psi\rangle$ is known as the biorthogonal or Schmidt decomposition.

We begin by specifying the measurement that Alice must do on her system in order to have her statistics of possible updates given by the convex decomposition $\{(q_k, \sigma_k)\}$ of ρ. If the POVM on Bob's system that generates this decomposition is denoted by $\{E_k\}$, so that

$$q_k \sigma_k = \sqrt{\rho} E_k \sqrt{\rho},$$

and U is the unitary map that satisfies

$$|f_j\rangle = U |e_j\rangle,$$

then the required measurement on Alice's system is the one associated with the POVM $\{U E_k U^\dagger\}_{k=1}^n$. The proof is as follows.

The entangled state Alice and Bob share can be written in terms of U as

$$|\psi\rangle = \sum_j \sqrt{\lambda_j} U |e_j\rangle \otimes |e_j\rangle.$$

Upon measuring the POVM $\{U E_k U^\dagger\}$ on her system and obtaining outcome k, the projection postulate for POVMs dictates that Alice should describe Bob's system by the unnormalized state

$$\begin{aligned}
&\mathrm{Tr}_A \left(\sqrt{U E_k U^\dagger} |\psi\rangle\langle\psi| \sqrt{U E_k U^\dagger} \right) \\
&= \Big(\sum_j \sqrt{\lambda_j} |e_j\rangle\langle e_j| \Big) E_k \Big(\sum_{j'} \sqrt{\lambda_{j'}} |e_{j'}\rangle\langle e_{j'}| \Big) \\
&= \sqrt{\rho} E_k \sqrt{\rho} \\
&= q_k \sigma_k.
\end{aligned}$$

So after this measurement, with probability q_k Alice updates the density operator with which she describes Bob's system to σ_k.

It is also easy to show that the statistics of possible updates are given by *some* convex decomposition of ρ for *every* measurement Alice can do. This follows from the fact that every measurement on Alice's system can be described by a POVM of the form $\{UE_kU^\dagger\}$ for some choice of $\{E_k\}$ given a particular U. $\square$

When Alice entangles the system she submits to Bob with a system she keeps in her possession in such a way that Bob's reduced density operator is ρ, we shall say that Alice *submits* ρ to Bob. When Alice performs a measurement that leads to her statistics of possible updates being given by the convex decomposition $\{(q_k,\sigma_k)\}$ of ρ, we shall say that Alice *realizes* this decomposition on Bob's system.

IV. THE NATURE OF THE OPTIMIZATION PROBLEM

In section II.D, we formulated the problem of determining the optimal cheat strategy for Alice as a variational problem over the entangled state that she initially prepares and the measurements she performs on her half of the system. However, from the results of the section III.C it is clear that in determining Alice's probability of unveiling the bit of her choosing, all that is important about the entangled state she prepares is the reduced density operator ρ she submits to Bob, and all that is important about the measurement she performs is the convex decomposition of ρ that she thereby realizes. It suffices therefore to vary over ρ and its convex decompositions.

We begin by showing that if Alice is attempting to unveil a bit b then it suffices for her to realize a convex decomposition with a number of elements less than or equal to n_b. The proof is as follows. Suppose Alice realizes a convex decomposition $\{(\tilde{q}_j,\tilde{\sigma}_j)\}_{j=1}^{n'}$ with a number of elements n' that is greater than n_b. She still must announce to Bob an index between 1 and n_b, so that the elements of this decomposition must be grouped into n_b sets, where elements in the kth set, S_k, correspond to announcing the index k to Bob. When Alice announces index k, Bob will measure the projector $\left|\psi_k^b\right\rangle\left\langle\psi_k^b\right|$ and obtain a positive result with probability $\sum_{j\in S_k}\tilde{q}_j\left\langle\psi_k^b\right|\tilde{\sigma}_j\left|\psi_k^b\right\rangle$. However, there is always an n_b-element convex decomposition that yields the same probability of a positive result as the one considered here; specifically, the decomposition $\{(q_k,\sigma_k)\}_{k=1}^{n_b}$ with $q_k\sigma_k=\sum_{j\in S_k}\tilde{q}_j\tilde{\sigma}_j$.

It follows that the probability of Alice succeeding at unveiling the bit b given that she submits ρ and realizes a convex decomposition $\{(q_k,\sigma_k)\}_{k=1}^{n_b}$ of ρ is

$$P_{Ub}=\sum_{k=1}^{n_b} q_k\left\langle\psi_k^b\right|\sigma_k\left|\psi_k^b\right\rangle. \tag{4}$$

Thus, if Alice submits ρ and realizes the convex decompositions $\left\{\left(q_k^0,\sigma_k^0\right)\right\}_{k=1}^{n_0}$ and $\left\{\left(q_k^1,\sigma_k^1\right)\right\}_{k=1}^{n_1}$ to unveil bit values of 0 and 1 respectively, then if she is equally likely to wish to unveil 0 as 1 (as we are assuming in this paper), her probability of unveiling the bit of her choosing is

$$\begin{aligned} P_U &= \frac{1}{2}P_{U0}+\frac{1}{2}P_{U1} \\ &= \frac{1}{2}\sum_{b=0}^{1}\sum_{k=1}^{n_b} q_k^b\left\langle\psi_k^b\right|\sigma_k^b\left|\psi_k^b\right\rangle. \end{aligned} \tag{5}$$

The task is to maximize P_U with respect to variations in ρ, $\left\{\left(q_k^0,\sigma_k^0\right)\right\}_{k=1}^{n_0}$ and $\left\{\left(q_k^1,\sigma_k^1\right)\right\}_{k=1}^{n_0}$ subject to the constraint that $\rho=\sum_{k=1}^{n_0}q_k^0\sigma_k^0=\sum_{k=1}^{n_1}q_k^1\sigma_k^1$.

It is useful to divide this optimization problem into two steps. In the first step one determines, for an arbitrary but fixed ρ, the n_b-element convex decomposition of ρ that maximizes the probability P_{Ub} of Alice unveiling the bit b. Given this solution, the probability P_U of Alice unveiling the bit of her choosing can be expressed entirely in terms of the submitted ρ. In the second step one determines the ρ that maximizes P_U.

V. RESULTS FOR GENERAL PROTOCOLS

A. The connection to state estimation

We will show that the problem of optimizing the convex decomposition for an arbitrary but fixed density operator has an intimate connection to the problem of optimal state estimation. As discussed in section III.B, for every convex decomposition $\{(q_k,\sigma_k)\}_k$ there exists a POVM $\{E_k\}$, defined over the support of ρ, that generates this decomposition as in Eq.(3). Thus, Eq.(4) can be written as

$$P_{Ub}=\sum_{k=1}^{n_b}\left\langle\psi_k^b\right|\sqrt{\rho}E_k\sqrt{\rho}\left|\psi_k^b\right\rangle.$$

A set of normalized states $\{\chi_k^b\}$ and probabilities $\{w_k^b\}$ can be defined in terms of ρ and $\{\psi_k^b\}$ as follows:

$$\left|\chi_k^b\right\rangle=\frac{\sqrt{\rho}\left|\psi_k^b\right\rangle}{\sqrt{\left\langle\psi_k^b\right|\rho\left|\psi_k^b\right\rangle}}, \tag{6}$$

$$w_k^b=\frac{\left\langle\psi_k^b\right|\rho\left|\psi_k^b\right\rangle}{\sum_k\left\langle\psi_k^b\right|\rho\left|\psi_k^b\right\rangle}. \tag{7}$$

In terms of these, P_{Ub} has the form

$$P_{Ub}=C\sum_{k=1}^{n_b}w_k^b\left\langle\chi_k^b\right|E_k\left|\chi_k^b\right\rangle,$$

where $C=\sum_k\left\langle\psi_k^b\right|\rho\left|\psi_k^b\right\rangle$.

We now recall [2] the problem of estimating the state of a system that is known to have been prepared in one of n_b states $\{\chi_k^b\}$ with prior probabilities $\{w_k^b\}$. The most general type of measurement is a POVM measurement, and it suffices to consider POVMs that have n_b elements (this is established by an argument exactly analogous to the one provided above for the sufficiency of n_b-element decompositions in optmizing over coherent attacks). For a measurement of the POVM $\{E_k\}$, the probability of estimating correctly is $\sum_{k=1}^{n} w_k^b \left\langle \chi_k^b \right| E_k \left| \chi_k^b \right\rangle$.

The connection between our problem and the state estimation problem is now clear. If $\{\chi_k^b\}$ and $\{w_k^b\}$ are defined by Eqs. (6) and (7), and $\{E_k\}$ is defined by (3), then the following relation holds. The probability of unveiling a bit b, associated with a set of states $\left\{\psi_k^b\right\}$, when Bob's reduced density operator is ρ, given that Alice's strategy consists of realizing an n_b-element convex decomposition $\{(q_k, \sigma_k)\}$ of ρ, is a constant multiple of the probability of correctly estimating the state of a system, known to be prepared in one of n_b states $\{\chi_k^b\}$ with prior probabilities $\{w_k^b\}$, given a measurement of the POVM $\{E_k\}$.

So, if one has the solution to the problem of finding the POVM that maximizes the probability of correctly estimating the state of a system from among a set of pure states, then one also has the solution to the problem of finding the convex decomposition of ρ that Alice should realize to maximize her probability of passing Bob's test. There is a *duality* between these two information theoretic tasks.

This result is very useful since it connects a task about which very little is known to one about which a great deal is known. In particular, one is able to infer some general features of the optimal cheat strategy by appealing to some well-known theorems on state estimation.

One such feature is that if the $\left\{\psi_k^b\right\}$ are linearly independent, and the support of ρ is the span of the $\left\{\psi_k^b\right\}$, then the optimal convex decomposition of ρ is extremal. The proof is as follows. If the $\left\{\psi_k^b\right\}$ are linearly independent and span the support of ρ, then the $\left\{\chi_k^b\right\}$ are linearly independent. It is well known that in estimating a state drawn from a set of linearly independent states, the optimal POVM has elements of rank 1 [2]. The convex decomposition that is associated with such a POVM has elements that are pure states, *i.e.*, it is extremal.

B. The support of the optimal density operator

We now turn to the problem of determining the optimal density operator for Alice to submit to Bob. We begin by showing that although Alice could cheat by submitting a system with more degrees of freedom than the honest protocol specifies, she gains no advantage by doing so. In other words, the optimal ρ has a support that is equal to or a subspace of the span of $\left\{\psi_k^0\right\}_{k=1}^{n_0} \cup \left\{\psi_k^1\right\}_{k=1}^{n_1}$. We establish this by showing that for any ρ^* that has support strictly greater than this span, there is a ρ that has support that is equal to or a subspace of this span and that yields a greater value of P_U. Suppose the optimal convex decomposition of ρ^* for unveiling bit b is denoted $\left\{\left(q_k^{b*}, \sigma_k^{b*}\right)\right\}_{k=1}^{n_b}$. The maximum probability of Alice unveiling the bit of her choosing using ρ^* is then

$$P_U^{\max}\left(\rho^*\right) = \frac{1}{2}\sum_{b=0}^{1}\sum_{k=1}^{n_b} \left\langle \psi_k^b \right| q_k^{b*}\sigma_k^{b*} \left| \psi_k^b \right\rangle .$$

However, if Alice submits the density operator

$$\rho = G\rho^* G/\mathrm{Tr}\left(\rho^* G\right),$$

where G is the projector onto the span of $\left\{\psi_k^0\right\}_{k=1}^{n_0} \cup \left\{\psi_k^1\right\}_{k=1}^{n_1}$, and realizes the convex decomposition $\left\{\left(q_k^b, \sigma_k^b\right)\right\}_{k=1}^{n_b}$ defined by $q_k^b\sigma_k^b = Gq_k^{b*}\sigma_k^{b*}G/\mathrm{Tr}\left(\rho^* G\right)$, then her probability of unveiling whatever bit she desires is

$$P_U\left(\rho\right) = P_U^{\max}\left(\rho^*\right)/\mathrm{Tr}\left(\rho^* G\right).$$

Since $\mathrm{Tr}\left(\rho^* G\right) < 1$, it follows that $P_U\left(\rho\right) > P_U^{\max}\left(\rho^*\right)$.

C. Conditions for unveiling with certainty

Finally, we consider the question of whether, for a particular protocol, Alice can unveil the bit of her choosing with certainty. The necessary and sufficient condition for there to be a strategy that makes $P_{Ub} = 1$ for a given b, is that ρ is decomposed by the set of states $\left\{\psi_k^b\right\}_{k=1}^{n_b}$, that is, there must exist a probability distribution $\left\{q_k^b\right\}_{k=1}^{n_b}$ such that $\left\{\left(q_k^b, \left|\psi_k^b\right\rangle\left\langle\psi_k^b\right|\right)\right\}_{k=1}^{n_b}$ forms a convex decomposition of ρ. The necessary and sufficient condition for there to be a strategy that makes $P_U = 1$ is that there exists a ρ that is decomposed by both $\left\{\psi_k^0\right\}_{k=1}^{n_0}$ and $\left\{\psi_k^1\right\}_{k=1}^{n_1}$. In the terminology of section III.A, $\left\{\psi_k^0\right\}_{k=1}^{n_0}$ and $\left\{\psi_k^1\right\}_{k=1}^{n_1}$ must be composably coincident.

The results described in this section constitute all that we shall say about the optimal cheat strategy for an arbitrary protocol. For the rest of this paper, we shall restrict ourselves to the special case of sets $\left\{\psi_k^0\right\}_{k=1}^{n_0}$ and $\left\{\psi_k^1\right\}_{k=1}^{n_1}$ whose union span at most a two dimensional Hilbert space, that is, protocols that can be implemented using a single qubit.

VI. RESULTS FOR QUBIT PROTOCOLS

A. The Bloch ball representation

Our optimization problem is greatly simplified in the case of a 2D Hilbert space since there is a one-to-one mapping between the set of all density operators in such a space and the set of all points within the unit ball of

$\mathbb{R}^3$. For clarity, we begin by reminding the reader about the details of this mapping.

If one defines an inner product between operators A and B by $\mathrm{Tr}\left(A^\dagger B\right)$, the set of operators over a Hilbert space forms an inner product space. In a 2d Hilbert space, a particularly convenient orthogonal basis for the set of operators is the set of Pauli operators $\{\sigma_x, \sigma_y, \sigma_z, I\}$, with matrix representations in the $\{|0\rangle, |1\rangle\}$ basis of

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Any operator A can therefore be written as $A = \frac{1}{2}\left(a_0 I + \vec{a}\cdot\vec{\sigma}\right)$ where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ and $\vec{a} = (a_x, a_y, a_z)$, with $a_0, a_x, a_y, a_z \in \mathbb{C}^1$. In particular, for a density operator ρ, the constraints of unit trace ($\mathrm{Tr}(\rho) = 1$) and positivity ($\det(\rho) \geq 0$) imply that

$$\rho = \frac{1}{2}\left(I + \vec{r}\cdot\vec{\sigma}\right),$$
$$\text{where } \vec{r} \in \mathbb{R}^3 \text{ and } |\vec{r}| \leq 1.$$

Thus we see that every density operator is represented by a vector $\vec{r}$ within the unit ball of $\mathbb{R}^3$, which we shall refer to as the Bloch ball.[5]

Density operators describing pure states are characterized by a vanishing determinant, $\det(\rho) = 0$, which corresponds to a vector of unit length, $|\vec{r}| = 1$ that we shall sometimes denote by $\hat{r}$. Thus, pure states are represented by the points on the surface of the ball. The completely mixed state, $\rho = \frac{1}{2}I$, is represented by $\vec{r} = \vec{0}$, which is the point at the centre of the ball. If two density operators ρ_1 and ρ_2 are represented by vectors $\vec{r}_1$ and $\vec{r}_2$, the inner product between ρ_1 and ρ_2 is given by $\mathrm{Tr}(\rho_1\rho_2) = \frac{1}{2}\left(1 + \vec{r}_1\cdot\vec{r}_2\right)$. It follows that orthogonal states are represented by antipodal points, since $\mathrm{Tr}(\rho_1\rho_2) = 0$ implies $\vec{r}_1\cdot\vec{r}_2 = -1$.

We are now in a position to obtain a representation on the Bloch ball of all the density operators that can be formed by convex combination of a particular set of elements $\{\sigma_k\}_{k=1}^n$, that is, all the ρ that have the form

$$\rho = \sum_{k=1}^n q_k \sigma_k$$

for some probability distribution $\{q_k\}_{k=1}^n$. Since the set of density operators that can be formed by an arbitrary set of elements $\{\sigma_k\}_{k=1}^n$ is the same as the set that can be formed by an uncontractable set of elements from which all the states in $\{\sigma_k\}_{k=1}^n$ can be built up by convex combination, it suffices to consider only uncontractable sets of elements.

Denoting the Bloch vectors associated with ρ and σ_k by $\vec{r}$ and $\vec{s}_k$ respectively, we find the relevant set to be given by

$$\vec{r} = \sum_{k=1}^n q_k \vec{s}_k, \text{ where } 0 \leq q_k \leq 1, \ \sum_{k=1}^n q_k = 1.$$

To understand what this manifold of points looks like, consider the simplest case of $n = 2$. The above equation can then be written as

$$\vec{r} = \vec{s}_1 + \lambda\left(\vec{s}_2 - \vec{s}_1\right), \text{ where } 0 \leq \lambda \leq 1.$$

This is simply the parametric equation for a segment of a straight line extending between $\vec{s}_1$ and $\vec{s}_2$. Similarly, in the case of $n = 3$, we have

$$\vec{r} = \vec{s}_1 + \lambda\left(\vec{s}_2 - \vec{s}_1\right) + \xi\left(\vec{s}_3 - \vec{s}_2\right),$$

where $0 \leq \lambda \leq 1$ and $0 \leq \xi \leq \lambda$.

Since σ_1, σ_2 and σ_3 were assumed to form an uncontractable set of elements, $\vec{s}_1$, $\vec{s}_2$ and $\vec{s}_3$ cannot lie on a line, and therefore define the vertices of a triangle. The above equation is the parametric equation for the surface of points inside this triangle. For $n = 4$, we have

$$\vec{r} = \vec{s}_1 + \lambda\left(\vec{s}_2 - \vec{s}_1\right) + \xi\left(\vec{s}_3 - \vec{s}_2\right) + \zeta\left(\vec{s}_4 - \vec{s}_3\right),$$

where $0 \leq \lambda \leq 1$, $0 \leq \xi \leq \lambda$ and $0 \leq \zeta \leq \xi$.

Again, since σ_1, σ_2, σ_3 and σ_4 were assumed to form an uncontractable set of elements, none of $\vec{s}_1$, $\vec{s}_2$, $\vec{s}_3$ or $\vec{s}_4$ can lie along the line segment defined by any other two, nor inside the surface of the triangle defined by any other three, and thus these vectors define the vertices of either a convex quadrilateral or a tetrahedron. The above equation is the parametric equation for the surface of points inside this quadrilateral, or the volume of points inside this tetrahedron. Similarly, for greater than 4 uncontractable elements, we obtain the parametric equation for the points inside an n-vertex convex polygon or convex polyhedron. All told, in the case of a set of n uncontractable elements, the set of density operators that can be composed from these will be represented by the region inside an n-vertex convex polytope. A few different sets of states and the density operators that can be composed from them are depicted in Fig.1.

[5]The surface of the ball is usually referred to as the Bloch sphere or the Riemann sphere in the context of spins, and the Poincare sphere in the context of photon polarization.

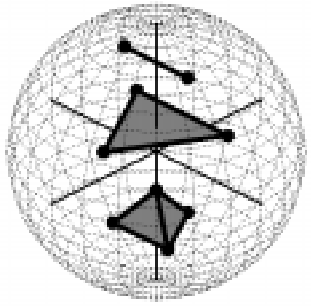

Fig.1 *A depiction of three sets of states containing 2, 3 and 4 elements respectively. The points in the Bloch ball representing these states are indicated by small black spheres. The manifolds inside the line segment, triangle and tetrahedron that are defined by each set of points represent all the density operators that can be composed with each set of states.*

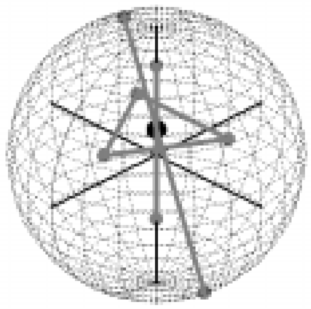

Fig.2 *An illustration of three convex decompositions of a fixed density operator, two of which are 2-element decompositions, and one of which is a 3-element decomposition. The point in the Bloch ball representing the density operator is indicated with a large black sphere. Each convex decomposition is represented by a polytope containing the point representing the density operator, the vertices of which represent the elements of the decomposition. These are indicated in grey. The longer of the two line segments, which has its vertices on the surface of the Bloch ball, is an example of an extremal convex decomposition.*

It is now easy to see the solution to a complementary problem, namely, how to obtain a representation on the Bloch ball of all the uncontractable convex decompositions of a particular density operator ρ. If ρ is represented by the point $\vec{r}$, then every n-element uncontractable convex decomposition of ρ is represented by an n-vertex convex polytope which contains $\vec{r}$. For instance, every 2-element uncontractable convex decomposition of ρ is represented by a line segment that contains $\vec{r}$; every 3-element uncontractable convex decomposition of ρ is represented by a triangle that contains $\vec{r}$, and so forth. In Fig.2, we illustrate a few of the convex decompositions of a fixed density operator.

Of particular interest to us in the present context are *extremal* convex decompositions of a density operator ρ (which are always uncontractable). Since pure states are associated with unit Bloch vectors, the convex polytopes associated with such decompositions have their vertices on the surface of the Bloch ball. Fig.2 provides an example of this distinction.

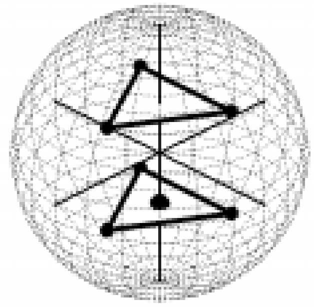

Fig.3 *A depiction of a fixed density operator and two sets of states, the lower of which decomposes the density operator and the uppermost of which does not.*

B. The conditions under which Alice can unveil the bit of her choosing with certainty

In section V.C it was pointed out that a strategy with $P_{Ub}=1$ exists if and only if ρ is decomposed by the states $\left\{\psi_k^b\right\}_{k=1}^n$. The Bloch ball representation gives a simple way of testing whether this condition is satisfied for protocols restricted to a 2D Hilbert space. It suffices to plot the convex polytope whose vertices are the points representing the $\left\{\psi_k^b\right\}_{k=1}^n$ and to determine whether the point representing ρ is contained in this polytope or not. If it is, then Alice can unveil bit b with certainty. If it is not, then she cannot. An example of the two possibilities is provided in Fig.3.

More importantly, we can now answer the question of whether there exists a strategy for Alice with $P_U=1$ for protocols restricted to a 2D Hilbert space. As pointed out in section V.C this only occurs if the two sets of states are composably coincident. It is clear now how to verify whether this is the case or not. Simply plot the convex polytopes associated with both sets of states, and determine whether they intersect one another or not. If they do, then any point inside the region of intersection corresponds to a density operator that is decomposed by both sets and consequently lets Alice unveil the bit of her choosing with probability 1. If they do not, then this probability is strictly less than 1.

The convex polytopes associated with the sets of states used in the BB84 BC protocol are depicted in Fig.4. Since these cross at the origin, it follows that if Alice submits to Bob the completely mixed state, she can achieve $P_U=1$. So we simply have a restatement of the fact that if Alice initially prepares a maximally entangled state, such as the EPR state, and submits half to Bob, then she can achieve $P_U=1$. The protocols we shall consider in the rest of this paper are associated with non-intersecting convex polytopes. See Figs. 6-10 for examples.

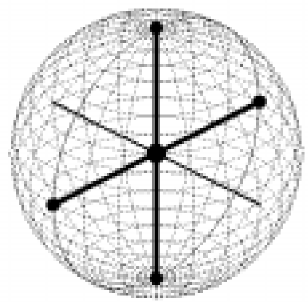

Fig.4. *The Bloch ball representation of the BB84 BC protocol. Since the polytopes representing the sets of states defined by the protocol intersect, Alice can submit the density operator associated with their intersection to make her probability of unveiling whatever bit she desires equal to unity.*

C. Optimizing over the convex decompositions of an arbitrary but fixed density operator

We now turn to the problem of determining the optimal EPR cheating strategy for a qubit protocol. We do not solve this problem completely; rather, we solve it under the further restriction that each set contains only linearly independent states. In the present 2D context, linear independence implies that each set can have no more than two elements.

As discussed in section IV, it is useful to split the problem into two parts involving optimization over convex decompositions of an arbitrary but fixed density operator, followed by optimization over density operators. We address these two parts of the problem in this section and the next section respectively.

We begin with the problem of maximizing the probability, P_{Ub}, that Alice can unveil the bit b given that she submitted a density operator ρ. This maximum must be found with respect to variations in the convex decomposition of ρ that she realizes. The optimal decomposition will depend on ρ and the states in the set $\{\psi_k^b\}_{k=1}^{n_b}$. In order to simplify the notation in this section, we drop the index b from $|\psi_k^b\rangle$ and n_b. We also assume that ρ is impure, since otherwise there is no optimization problem to be solved.

1. A set containing one element ($n=1$)

In this case, Bob's test is fixed (he always measures the projector onto $|\psi_1\rangle$), so the probability of passing this test depends only on ρ and not on the convex decomposition of ρ that Alice realizes. Thus, there is no optimization over decompositions to be performed in this case.

2. A set containing two elements ($n=2$)

Let the Bloch vectors associated with $|\psi_k\rangle$ and ρ be denoted by $\hat{a}_k$ and $\vec{r}$ respectively, and let those associated with the elements, σ_k, of the two-element convex decomposition $\{(q_k,\sigma_k)\}_{k=1}^{2}$ that Alice realizes be denoted by $\vec{s}_k$. In terms of these, Alice's probability of passing Bob's test, specified by Eq.(4), has the following form

$$P_{Ub} = \frac{1}{2}\left(1+\sum_{k=1}^{2} q_k\left(\hat{a}_k\cdot\vec{s}_k\right)\right). \tag{8}$$

We must maximize this subject to the constraint that $\vec{r}=\sum_k q_k\vec{s}_k$.

We find that the optimal convex decomposition of $\vec{r}$ is given by

$$\begin{aligned}\vec{s}_1^{\,\mathrm{opt}} &= \vec{r}+L_+\left(\vec{r}\right)\hat{d},\\ \vec{s}_2^{\,\mathrm{opt}} &= \vec{r}+L_-\left(\vec{r}\right)\hat{d},\end{aligned} \tag{9}$$

and

$$q_k^{\mathrm{opt}} = \frac{1}{2}\frac{1-|\vec{r}|^2}{1-\vec{r}\cdot\vec{s}_k^{\,\mathrm{opt}}} \tag{10}$$

where

$$L_\pm\left(\vec{r}\right) = -\vec{r}\cdot\hat{d}\pm\sqrt{1-|\vec{r}|^2+\left(\vec{r}\cdot\hat{d}\right)^2}, \tag{11}$$

and

$$\hat{d} = \frac{\hat{a}_1-\hat{a}_2}{|\hat{a}_1-\hat{a}_2|}. \tag{12}$$

Note that $\left|\vec{s}_1^{\,\mathrm{opt}}\right| = \left|\vec{s}_2^{\,\mathrm{opt}}\right| = 1$, which means that this is an extremal convex decomposition. The proof of optimality is presented in Appendix A.

This solution has a very simple geometrical description. It is the convex decomposition that is represented by the chord (*i.e.* line segment whose endpoints lie on the surface of the ball) that contains $\vec{r}$ and that is parallel to the chord defined by $\hat{a}_1$,$\hat{a}_2$. An example is presented in Fig.5.

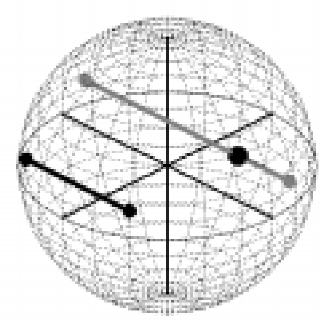

Fig.5. *An illustration of the optimal convex decomposition for Alice to realize when she has submitted to Bob a fixed density operator(indicated by the large black sphere) and is attempting to convince him that he has one of two states (indicated by the small black spheres). This is represented by the chord(indicated in grey) that is parallel to the chord defined by the two states. After Alice realizes this decomposition (by making a measurement on the system that is entangled with Bob's), she updates her description of Bob's system to whichever of the elements it happened to be collapsed to(indicated by the grey spheres). When it comes time for Alice to announce to Bob which of the two states he should test for to verify her honesty, she announces the state which has the smallest angular separation from the element of the decomposition onto which she has collapsed his system.*

The corresponding probability of passing Bob's test is simply

$$P_{Ub}^{\max} = \frac{1}{2}\left(1 + \left(\vec{r} + L_{+}\left(\vec{r}\right)\hat{d}\right)\cdot\hat{a}_1\right).$$

In Hilbert space language,

$$P_{Ub}^{\max} = \frac{1}{2}\left(\langle\psi_1|\rho|\psi_1\rangle + \langle\psi_2|\rho|\psi_2\rangle\right) + \sqrt{2\left(1-\mathrm{Tr}(\rho^2)\right)|\langle\psi_1|\psi_2\rangle|^2 + \left(\langle\psi_1|\rho|\psi_1\rangle - \langle\psi_2|\rho|\psi_2\rangle\right)^2}.$$

D. Optimizing over density operators

We now consider the problem of determining the optimal density operator ρ for Alice to submit to Bob in order to maximize her probability of unveiling the bit of her choosing. The solution will depend on the values of n_0 and n_1. Given that we are assuming that the states in the sets $\left\{\psi_k^0\right\}_{k=1}^{n_0}$ and $\left\{\psi_k^1\right\}_{k=1}^{n_1}$ are linearly independent, there are only three possibilities to address: both sets contain two elements; one set contains two elements and the other contains one element; both sets contain one element. We shall consider each of these in turn.

1. Both sets contain two elements ($n_0 = n_1 = 2$)

Denote the Bloch vector associated with the state $\left|\psi_k^b\right\rangle$ by $\hat{a}_k^b$. The result of the previous section indicates that whatever the optimal $\vec{r}$ is, the optimal convex decomposition for unveiling bit b is represented by the chord passing through $\vec{r}$ parallel to the chord defined by $\hat{a}_1^b, \hat{a}_2^b$. We therefore have that Alice's probability of unveiling the bit of her choosing given an arbitrary $\vec{r}$ and given that when she attempts to unveil the bit b she realizes the convex decomposition of $\vec{r}$ that is optimal for doing so, is simply

$$P_U = \sum_{b=0}^{1}\frac{1}{4}\left(1 + \left(\vec{r} + L_{b+}\left(\vec{r}\right)\hat{d}_b\right)\cdot\hat{a}_1^b\right), \tag{13}$$

where $\hat{d}_b = \frac{\hat{a}_1^b - \hat{a}_2^b}{\left|\hat{a}_1^b - \hat{a}_2^b\right|}$ and

$$L_{b+}\left(\vec{r}\right) = -\vec{r}\cdot\hat{d}_b + \sqrt{1 - \left|\vec{r}\right|^2 + \left(\vec{r}\cdot\hat{d}_b\right)^2}.$$

It will be convenient to adopt the convention that the states in the protocol are indexed in such a way that $\left\langle\psi_1^0|\psi_1^1\right\rangle = \max_{k,k'}\left\langle\psi_k^0|\psi_{k'}^1\right\rangle$. In terms of the Bloch ball, the convention states that if one draws the chords defined by $\hat{a}_1^0, \hat{a}_2^0$ and $\hat{a}_1^1, \hat{a}_2^1$, the endpoints $\hat{a}_1^0$ and $\hat{a}_1^1$ have the smallest separation.

We consider two cases.

Case 1: The chords defined by $\hat{a}_1^0, \hat{a}_2^0$ and $\hat{a}_1^1, \hat{a}_2^1$ are parallel.

In this case $\hat{d}_0 = \hat{d}_1$ and there are a family of optimal $\vec{r}$'s satisfying the parametric equation

$$\vec{r}^{\text{opt}} = \frac{\hat{a}_1^0 + \hat{a}_1^1}{\left|\hat{a}_1^0 + \hat{a}_1^1\right|} + \lambda\hat{d}_0, \text{ for } 0 \leq \lambda \leq 2\frac{\hat{a}_1^0 + \hat{a}_1^1}{\left|\hat{a}_1^0 + \hat{a}_1^1\right|}\cdot\hat{d}_0. \tag{14}$$

This family corresponds to the points on the chord of the Bloch ball that is parallel to the chord defined by $\hat{a}_1^0, \hat{a}_2^0$ (or $\hat{a}_1^1, \hat{a}_2^1$) and that passes through the point on the surface of the ball that is equidistant between $\hat{a}_1^0$ and $\hat{a}_1^1$. This is illustrated in Fig.7.

Case 2: The chords defined by $\hat{a}_1^0, \hat{a}_2^0$ and $\hat{a}_1^1, \hat{a}_2^1$ are not parallel.

In this case, the optimal $\vec{r}$ is unique and is given by

$$\vec{r}^{\text{opt}} = \begin{cases} \vec{r}^{\max} \text{ if } \left|\vec{r}^{\max}\right| \leq 1 \\ \frac{\hat{a}_1^0 + \hat{a}_1^1}{\left|\hat{a}_1^0 + \hat{a}_1^1\right|} \text{ otherwise} \end{cases}, \tag{15}$$

where

$$\vec{r}^{\max} = x_0^{\max}\hat{d}_1^{\perp} + x_1^{\max}\hat{d}_0^{\perp} + x_2^{\max}\hat{n}. \tag{16}$$

Here

$$\begin{aligned} x_0^{\max} &= \frac{1}{\gamma_1}\hat{a}_1^1\cdot\hat{d}_1^{\perp}\sqrt{1-\left(x_2^{\max}\right)^2}, \\ x_1^{\max} &= \frac{1}{\gamma_0}\hat{a}_1^0\cdot\hat{d}_0^{\perp}\sqrt{1-\left(x_2^{\max}\right)^2}, \\ x_2^{\max} &= \frac{\left(\hat{a}_1^0 + \hat{a}_1^1\right)\cdot\hat{n}}{\sqrt{\left(\left(\hat{a}_1^0 + \hat{a}_1^1\right)\cdot\hat{n}\right)^2 + \left(\gamma_0+\gamma_1\right)^2}}, \end{aligned} \tag{17}$$

where $\gamma_b = \sqrt{1 - \left(\hat{a}_1^b\cdot\hat{n}\right)^2}$ and where

$$\begin{aligned} \hat{n} &= \hat{d}_0 \times \hat{d}_1, \\ \hat{d}_b^{\perp} &= \hat{d}_b \times \hat{n}, \\ \hat{d}_b &= \frac{\hat{a}_1^b - \hat{a}_2^b}{\left|\hat{a}_1^b - \hat{a}_2^b\right|}. \end{aligned} \tag{18}$$

Thus, the solution has one of two forms depending on whether the condition $|\vec{r}^{\max}| \leq 1$ holds or not. If it does not hold, then $\vec{r}^{\text{opt}} = \left(\hat{a}_1^0 + \hat{a}_1^1\right) / \left|\hat{a}_1^0 + \hat{a}_1^1\right|$, which is simply the point on the surface of the Bloch ball that is equidistant between $\hat{a}_1^0$ and $\hat{a}_1^1$ along the geodesic which connects them (recall that in our labelling convention $\hat{a}_1^0$ and $\hat{a}_1^1$ are the closest endpoints of the chords defined by $\hat{a}_1^0, \hat{a}_2^0$ and $\hat{a}_1^1, \hat{a}_2^1$). Fig.6 provides an example of a BC protocol where this is the case. If the condition $|\vec{r}^{\max}| \leq 1$ *does* hold, then $\vec{r}^{\text{opt}} = \vec{r}^{\max}$. We will not attempt to provide a geometrical description of this point in the general case, however Figs. 4 and 9 provide simple examples of BC protocols where $|\vec{r}^{\max}| \leq 1$.

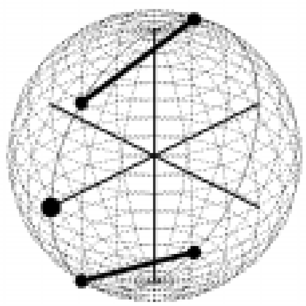

Fig.6. *A BC protocol where the two sets of states are represented by chords that lie in a plane, but which do not intersect inside the Bloch ball. The optimal density operator is represented by the point that lies equidistant between the two closest chord endpoints on the geodesic which connects them.*

In situations having a high degree of symmetry, one can easily deduce some of the features of $\vec{r}^{\text{opt}}$. We present a few such cases.

Case 2.1: If the chord defined by $\hat{a}_1^0$ and $\hat{a}_2^0$ and the chord defined by $\hat{a}_1^1$ and $\hat{a}_2^1$ lie in a plane, then $\vec{r}^{\max}$ is the point of intersection of the lines containing these chords. If this point falls inside the Bloch ball ($|\vec{r}^{\max}| \leq 1$), then it represents the optimal density operator. This confirms the results of section V.C. The BB84 BC protocol, illustrated in Fig.4, is an instance of such a case. If the point of intersection falls outside the Bloch ball ($|\vec{r}^{\max}| > 1$), then the optimal density operator is as described above. The BC protocol that is illustrated in Fig.6 is an instance of such a case.

Case 2.2: If the chord defined by $\hat{a}_1^0$ and $\hat{a}_2^0$ and the chord defined by $\hat{a}_1^1$ and $\hat{a}_2^1$ both pass through the $\hat{n}$ axis, then $\vec{r}^{\text{opt}}$ lies along this axis.

Case 2.3: If the chord defined by $\hat{a}_1^0$ and $\hat{a}_2^0$ and the chord defined by $\hat{a}_1^1$ and $\hat{a}_2^1$ are parallel to, equidistant from, and on either side of the equatorial plane perpendicular to $\hat{n}$, then $\vec{r}^{\text{opt}}$ lies in that plane.

If the conditions of cases 2.2 and 2.3 both hold, then $\vec{r}^{\text{opt}}$ lies at the centre of the Bloch ball. This corresponds to Alice submitting the completely mixed state. An example of such a protocol is provided in Fig.9. Although in the example of this figure the two chords point in orthogonal directions, this is not necessary, it is only necessary that they not be parallel.

The proofs of the results of this section are presented in Appendix B.

2. *One set contains one element and one set contains two elements* ($n_0 = 1, n_1 = 2$)

We now assume that one of the sets $\left\{\psi_k^0\right\}_{k=1}^{n_0}$ and $\left\{\psi_k^1\right\}_{k=1}^{n_1}$ has only a single element while the other has two. Without loss of generality we may assume that the single element set is the $b = 0$ set, and we denote its unique element by $\left|\psi^0\right\rangle$. So in order to unveil a bit value of 1 Alice can announce either $k = 1$ or $k = 2$ and must then pass Bob's test for $\left|\psi_k^1\right\rangle$, while to unveil a bit value of 0 Alice has no choice but to pass a test for the state $\left|\psi^0\right\rangle$.

We first consider the case where $\left\langle\psi^0|\psi_1^1\right\rangle = \left\langle\psi^0|\psi_2^1\right\rangle$. This corresponds to case 1 of section VI.D.1 in the limit that $\hat{a}_1^0$ and $\hat{a}_2^0$ converge to a single point $\hat{a}^0$ representing $\left|\psi^0\right\rangle$. There is a family of optimal solutions of the form

$$\vec{r}^{\text{opt}} = \frac{\hat{a}^0 + \hat{a}_1^1}{|\hat{a}^0 + \hat{a}_1^1|} + \lambda\hat{d}_1, \text{ for } 0 \leq \lambda \leq 2.$$

This family corresponds to the points on the chord of the Bloch ball that is parallel to the chord defined by $\hat{a}_1^1, \hat{a}_2^1$ and that passes through the point on the surface of the ball that is equidistant between $\hat{a}^0$ and $\hat{a}_1^1$. The BC protocol illustrated in Fig.10 is an example of this case. The case $\left\langle\psi^0|\psi_1^1\right\rangle \neq \left\langle\psi^0|\psi_2^1\right\rangle$ corresponds to case 2 of section VI.D.1 in the limit that $\hat{a}_1^0$ and $\hat{a}_2^0$ converge to the point $\hat{a}^0$. In this limit, we find that $|\vec{r}^{\max}| > 1$. Consequently,

$$\vec{r}^{\text{opt}} = \frac{\hat{a}^0 + \hat{a}_1^1}{|\hat{a}^0 + \hat{a}_1^1|}.$$

3. *Both sets contain one element* ($n_0 = 1, n_1 = 1$)

We now assume there is only a single element in both of the sets, and denote each of these states by $\left|\psi^b\right\rangle$. Thus to unveil a bit value of b Alice must pass Bob's test for $\left|\psi^b\right\rangle$. Consider first the possibility that $\left|\psi^0\right\rangle$ and $\left|\psi^1\right\rangle$ are orthogonal. In this case, no matter what ρ Alice submits, her probability of unveiling either bit is strictly 1/2.

When $\left|\psi^0\right\rangle$ and $\left|\psi^1\right\rangle$ are not orthogonal, the situation corresponds to case 2 of section VI.D.1, in the limit that $\hat{a}_1^b$ and $\hat{a}_2^b$ converge to a single point $\hat{a}^b$. In this limit we again find $|\vec{r}^{\max}| > 1$. Consequently,

$$\vec{r}^{\text{opt}} = \frac{\hat{a}^0 + \hat{a}^1}{|\hat{a}^0 + \hat{a}^1|}.$$

An example is presented in Fig.8.

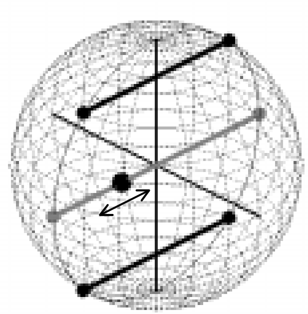

Fig.7. *An illustration of a BC protocol of the form proposed by Aharonov* et al. *[10]. The two sets of states are given by Eq. (19) with $\theta = \pi/8$. There is a family of optimal density operators lying along the chord indicated in grey.*

VII. APPLICATIONS OF THE RESULTS

These results can be applied to the generalized BB84 BC protocol proposed by Aharonov *et al.* [10]. The protocol is defined by the following states, from which an honest Alice chooses uniformly

$$\begin{aligned} \left|\psi_1^0\right\rangle &= |\theta\rangle\,, \ \left|\psi_2^0\right\rangle = |-\theta\rangle\,, \\ \left|\psi_1^1\right\rangle &= |\pi/2-\theta\rangle\,, \left|\psi_2^1\right\rangle = |\pi/2+\theta\rangle\,, \end{aligned} \tag{19}$$

where $|\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and θ is some fixed angle satisfying $0 < \theta \leq \frac{\pi}{4}$. The sets of states associated with bits 0 and 1 describe parallel chords on the Bloch ball, as depicted in Fig.7. We therefore have an instance of case 1 of section VI.D.1. It follows that an optimal strategy for Alice is to simply submit $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and tell Bob to test for $\left|\psi_1^b\right\rangle$, where b is the bit she wishes to unveil. Another is to submit $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and to tell Bob to test for $\left|\psi_2^b\right\rangle$. So Alice does not need to make use of entanglement in this case. The most general optimal strategy is for Alice to submit $\rho = w\,|+\rangle\langle+| + (1-w)\,|-\rangle\langle-|$, realize the convex decomposition $\{(w, |+\rangle\langle+|), ((1-w), |-\rangle\langle-|)\}$, and tell Bob to test for $\left|\psi_1^b\right\rangle$ $(\left|\psi_2^b\right\rangle)$ upon obtaining the outcome $|+\rangle$ $(|-\rangle)$. Alice's maximum probability of unveiling whatever bit she desires is

$$P_U^{\max} = \frac{1}{2}(1 + \sin 2\theta)\,.$$

Previously, the best known upper bound on this probability was $P_U \leq \frac{1}{2}\left(1 + \frac{1}{\cos^2 2\theta}\left(\sqrt{1+2\cos^2 2\theta} - 1\right)\right)$, as can be inferred from the results in section 5 of Ref. [10]. In the case of $\theta = \pi/8$, we find $P_U^{\max} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \simeq .85355$, while the previous best bound was $P_U \leq \frac{\sqrt{8}-1}{2} \simeq .91421$.

We can now compare this with Bob's maximal probability of estimating Alice's commitment correctly. If Alice follows the honest protocol for committing a bit b, she chooses uniformly between $\left|\psi_1^b\right\rangle$ and $\left|\psi_2^b\right\rangle$ and submits a system in this state. Bob must therefore discriminate between density operators ρ_0 and ρ_1 defined by $\rho_b = \frac{1}{2}\sum_{k=1}^2 \left|\psi_k^b\right\rangle\left\langle\psi_k^b\right|$. His maximum probability of doing so is given by Eq.(1), in this case,

$$P_E^{\max} = \frac{1}{2}(1 + \cos 2\theta)\,.$$

It is worth noting that the quantity $\frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1|$ appearing in Eq.(1) is simply half the Euclidean distance between the points in the Bloch ball representing ρ_0 and ρ_1.

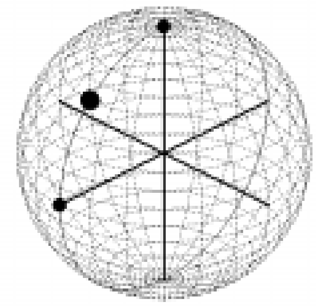

Fig.8. *An illustration of a BC protocol of the form specified in Eq. (21), with $\gamma = \pi/4$. The optimal density operator is indicated by the large black sphere. BC protocols of this form achieve the same trade-off between concealment and bindingness as those of the form proposed by Aharonov* et al.

From the above expression for $P_U^{\max}$ and $P_E^{\max}$, we can conclude that there is a trade-off between these quantities of the form

$$(P_U^{\max} - 1/2)^2 + (P_E^{\max} - 1/2)^2 = 1/4. \tag{20}$$

At $\theta = 0$, $P_E^{\max} = 1$ and $P_U^{\max} = 1/2$, so that there is no concealment against Bob, but perfect bindingness against Alice (since $P_U^{\max} = 1/2$ for an honest Alice). At $\theta = \pi/4$, $P_E^{\max} = 1/2$ and $P_U^{\max} = 1$, so that the roles of Alice and Bob are reversed. The only choice of θ leading to a 'fair' protocol is $\theta = \pi/8$. In this case, $P_E^{\max} = P_U^{\max} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$.

Our results also imply that the same trade-off between $P_U^{\max}$ and $P_E^{\max}$ can be achieved with the most simple imaginable BC protocol, namely one wherein Alice submits to Bob one of two non-orthogonal states. Specifically, to commit a bit b, an honest Alice sends Bob a qubit in the state $\left|\psi^b\right\rangle$, where

$$\begin{aligned} \left|\psi^0\right\rangle &= |0\rangle\,, \\ \left|\psi^1\right\rangle &= |\gamma\rangle\,, \end{aligned} \tag{21}$$

where γ is some fixed angle satisfying $0 < \gamma \leq \pi/2$. An example of this protocol is illustrated in Fig.8. This is an instance where $n_0 = 1$ and $n_1 = 1$, which was considered in section VI.D.3. One can infer from the results of that section that Alice's optimal strategy is to submit the state $|\gamma/2\rangle$ and to announce whatever bit she wishes to unveil. It is straightforward to verify that this protocol has the same properties as the one described above.

It is easy to understand the equivalence of these protocols geometrically. $P_U^{\max}$ is proportional to the cosine of the angular separation of the endpoints of the polytopes (chords or points) representing the sets of states an honest Alice chooses from. Meanwhile, $P_E^{\max}$ is proportional to the Euclidean distance between the midpoints of these polytopes. It is easy to see from Figs. 7 and 8 that if the endpoints have the same angular separation, then the midpoints have the same Euclidean separation.

Interestingly, it turns out that any protocol satisfying the conditions of cases 2.2 and 2.3 of section VI.D.1 *also* yields exactly the same trade-off between $P_U^{\max}$ and $P_E^{\max}$. Specifically, one can use any protocol of the form

$$\begin{aligned} \left|\psi_1^0\right\rangle &= |\theta, 0\rangle\,, \;\; \left|\psi_2^0\right\rangle = |-\theta, 0\rangle\,, \\ \left|\psi_1^1\right\rangle &= |\pi/2-\theta, \phi\rangle\,, \left|\psi_2^1\right\rangle = |\pi/2+\theta, -\phi\rangle\,, \end{aligned} \tag{22}$$

where $|\theta,\phi\rangle = \cos\theta\,|0\rangle + e^{i\phi}\sin\theta\,|1\rangle$ and θ and ϕ are fixed angles satisfying $0<\theta\leq\frac{\pi}{4}$, $0<\phi\leq\pi/2$. Fig.9 depicts an example of such a protocol. Geometrically, $P_U^{\max}$ is no longer given by the angle between the endpoints of the two polytopes representing the states an honest Alice chooses from but rather the angle between the endpoints of these polytopes and the closest endpoints of the polytopes representing the elements of the convex decomposition that Alice realizes. Nonetheless, the fact that the latter angle is simply half of the former angle ensures that $P_U^{\max}$ is the same. The only difference is that Alice's optimal strategy in this case requires the use of entanglement.

Finally, we consider a protocol wherein there is a single state associated with committing a bit 0 but two states associated with committing bit 1, specifically,

$$\begin{aligned} \left|\psi^0\right\rangle &= |0\rangle\,, \\ \left|\psi_1^1\right\rangle &= |\alpha\rangle\,, \left|\psi_2^1\right\rangle = |-\alpha\rangle\,, \end{aligned} \tag{23}$$

where α is some fixed angle satisfying $0<\alpha\leq\frac{\pi}{2}$. An example of this protocol is provided in Fig.10. It is of the form described in section VI.D.2, with $\left\langle\psi^0|\psi_1^1\right\rangle = \left\langle\psi^0|\psi_2^1\right\rangle$. From the results of that section, we can infer that there are a family of optimal coherent attacks of the following form. Alice submits a density operator of the form $\rho = w\,|\alpha/2\rangle\langle\alpha/2| + (1-w)\,|-\alpha/2\rangle\langle-\alpha/2|$. If she decides to try to unveil bit 0, she simply announces this to Bob. If she decides to try to unveil bit 1, she realizes the convex decomposition $\{(w, |\alpha/2\rangle\langle\alpha/2|), ((1-w), |-\alpha/2\rangle\langle-\alpha/2|)\}$, and upon obtaining the outcome $|\alpha/2\rangle$ ($|-\alpha/2\rangle$) tells Bob to test for $|\alpha\rangle$ ($|-\alpha\rangle$). Alice's maximum probability of unveiling whatever bit she desires in this case is

$$P_U^{\max} = \frac{1}{2} + \frac{1}{2}\cos\alpha.$$

Meanwhile, from Eq.(1), we can infer that Bob's maximum probability of correctly estimating Alice's commitment is

$$P_E^{\max} = \frac{1}{2} + \frac{1}{2}\sin^2\alpha.$$

The trade-off between $P_U^{\max}$ and $P_E^{\max}$ is

$$2\left(P_U^{\max} - \frac{1}{2}\right)^2 + \left(P_E^{\max} - \frac{1}{2}\right) = \frac{1}{2}. \tag{24}$$

A 'fair' protocol has $P_U^{\max} = P_E^{\max} = \frac{1}{2} + \frac{\sqrt{5}-1}{4} \simeq .80902$.

From a comparison of the trade-offs (19) and (24), it is easy to verify that a protocol which uses the states (23) achieves, for a given bindingness (a given $P_U^{\max}$), a concealment that is greater (and thus a $P_E^{\max}$ that is smaller) than the concealment that can be achieved in a protocol using the states (19), (21) or (22).

This point is easy to see geometrically. We compare the states (21) with the states (23) for simplicity. From an inspection of Figs. 8 and 10 it is easy to see that if the endpoints of the polytopes defined by the two protocols have the same angular separation, the midpoints do *not* have the same Euclidean separation - the separation is smaller for a BC protocol defined by the states (23).

An obvious question to ask at this point is whether the trade-off relation of Eq.(24) is optimal, in the sense that the concealment against Bob is maximized for a given bindingness against Alice. Elsewhere [7] we show that it *is* optimal among a certain class of protocols (which includes the generalized BB84 protocols) that can be implemented using a single qubit. It is also shown that a better trade-off can be achieved with a BC protocol that can be implemented using a single qu*trit*, that is, a three-level system. The protocol we suggest in Ref. [7] is not a generalized BB84 BC protocol, however, an equivalent protocol that *is* of the generalized BB84 form has been proposed by Ambainis [16].

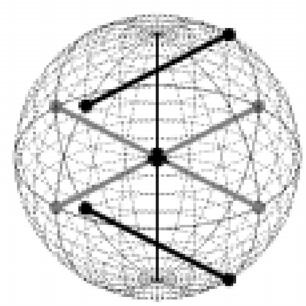

Fig.9. *An illustration of a BC protocol of the form specified in Eq. (22), with $\theta = \pi/8$ and $\phi = \pi$. The optimal density operator in this case lies at the origin. Depending on which bit Alice desires to unveil, she realizes the convex decomposition parallel to one or the other of the two chords.*

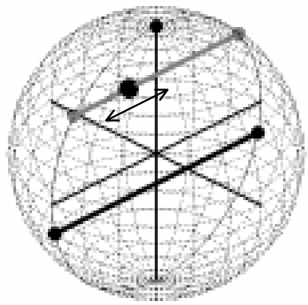

Fig.10. *An illustration of a BC protocol of the form specified in Eq. (23), with* $\alpha = \arccos\left((\sqrt{5}-1)/2\right)$. *There is a family of optimal density operators lying along the chord indicated in grey. BC protocols of this form achieve a better trade-off between concealment and bindingness than those of the form proposed by Aharonov* et al.

VIII. CONCLUSIONS

We have formulated the problem of optimizing coherent attacks on Generalized BB84 BC protocols in terms of a well known theorem of Hughston, Josza and Wootters. We have found that there is a mapping between this problem and one of state estimation. Specifically, we have shown that the convex decomposition of a fixed density operator that is optimal for successfully preparing one of a set of states is related in a simple way to the POVM measurement that is optimal for discriminating among certain transformations of these states.

We have identified Alice's optimal coherent attack for a class of generalized BB84 BC protocols that can be implemented using a single qubit. From these results we have determined the degree of bindingness that can be achieved in the BC protocol proposed by Aharonov *et al.*, improving upon the best previous upper bound. This enables us to identify the trade-off between the degree of concealment and the degree of bindingness for this protocol. It has also led us to identify several qubit protocols that achieve the same trade-off as the proposal of Aharonov *et al.* , as well as a qubit protocol that achieves a better trade-off.

In optimizing over Alice's strategies, we have relied on the Bloch ball representation of quantum states. This provides a convenient geometrical picture of a coherent attack. Although this representation can be generalized to higher dimensions [17], it is unlikely that such simple geometric pictures can be provided in the general case. In any event, there remain many questions to be answered even for qubit protocols, for which this approach is likely to provide some insight. For instance, one can use it to consider qubit BC protocols that are *not* generalizations of the BB84 BC protocol.

In another paper [7], we determine the optimal coherent attack in a class of BC protocols that is larger than the set of generalized BB84 protocols. However, the problem of determining the optimal trade-off between concealment and bindingness from among *all* BC protocols remains open.

Beyond their relevance to bit commitment, coherent attacks are interesting as an example of what might be considered a fundamental task in quantum information processing, namely, the preparation of quantum states at a remote location. One can define many variants of this task, depending on whether the parties at the two locations are cooperative or adversarial, and depending on the available resources, such as the number of classical or quantum bits that can be exchanged, and the amount of prior entanglement the parties share. Bennett *et al.* [18] have recently considered remote state preparation in the case of cooperative parties who share prior entanglement and a classical channel. In the type of remote state preparation we have considered in this paper, the parties are adversarial and although Alice makes use of a quantum channel, she does so at a time prior to knowing which state she is supposed to prepare.

It seems to us that the primitive of remote state preparation, construed in its most general sense, may be as fundamental as the primitive of state estimation and just as significant for the purposes of determining what sorts of information processing tasks can be successfully implemented using quantum primitives. The mapping discussed above between state estimation and the particular type of remote state preparation considered in this paper suggests that there may be other connections between these two problems. In future work, we hope to explore this analogy in more detail.

IX. ACKNOWLEDGMENTS

We gratefully acknowledge J. E. Sipe for useful discussions. This work was supported by the National Science and Engineering Research Council of Canada, the Austrian Science Foundation FWF, and the TMR programs of the European Union Project No. ERBFM-RXCT960087.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.

[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[3] C. A. Fuchs, *Distinguishability and Accessible Information in Quantum Theory,* Ph.D. thesis, University of New Mexico, Albuquerque, NM, 1996.

[4] D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997).

[5] H.-K. Lo and H. F. Chau, *Phys. Rev. Lett.* **78**, 3410 (1997).
[6] This assumes that the two parties occupy laboratories whose spatial dimensions are small compared to the separation between Alice and Bob. If this assumption does not hold, then relativistic constraints allow one to achieve a form of bit commitment, as demonstrated by A. Kent, *Phys. Rev. Lett.* **83**, 1447 (1999).
[7] R. W. Spekkens and T. Rudolph, quant-ph/0106019.
[8] H.-K. Lo and H. F. Chau, *Physica D*, **120,** 177 (1998).
[9] L. Hardy and A. Kent, quant-ph/9911043.
[10] D. Aharonov *et al.*, quant-ph/0004017.
[11] L. Goldenberg, L. Vaidman and S. Wiesner, *Phys. Rev. Lett.* **82**, 3356 (1999).
[12] L. P. Hughston, R. Josza and W. Wootters, *Phys. Lett. A* **183,** 14 (1993).
[13] E. T. Jaynes, *Phys. Rev.* **108,** 171 (1957).
[14] A. Peres, *Found. Phys.* **20,** 1441 (1990).
[15] G. Cassinelli, E. De Vito and A. Levrero, *J. Math. Analysis and Appl.* **210**, 475 (1997).
[16] A. Ambainis, 'A new protocol and lower bounds for quantum coin flipping', preprint (2000).
[17] F. T. Hioe and J. H. Eberly, Phys. Rev. Lett. **47**, 838 (1981); J. Schlienz and G. Mahler, Phys. Rev. A. **52**, 4396 (1995).
[18] C. H. Bennett *et al.*, quant-ph/0006044 (2000).

X. APPENDIX A

We here provide the proof of optimality of the convex decomposition specified by Eq.(9). First, we establish the applicability of Jaynes' rule, defined in Eq.(2), to the probabilities in the optimal convex decomposition. This requires showing that the optimal decomposition is an extremal decomposition with the number of positively-weighted elements equal to the rank of ρ.

This is trivial to see for a pure ρ. We now demonstrate it for an impure ρ. Because we have assumed that the $\{\psi_k\}_{k=1}^n$ are linearly independent, they span the whole 2D Hilbert space, and because ρ has rank 2, its support is the 2D Hilbert space. Thus, the $\{\psi_k\}_{k=1}^n$ are linearly independent and have a span that is equal to the support of ρ, which, as shown in section V.A by the mapping to the state estimation problem, is sufficient to establish that the optimal convex decomposition is an extremal decomposition. It was shown in section IV that the number of positively-weighted elements in the optimal convex decomposition is less than or equal to n. In the present case, $n=2$, so this number must be less than or equal to 2. However, since ρ is impure, every convex decompositions of ρ has *at least* 2 elements receiving non-zero probability. Thus, the number must be precisely 2, which is the rank of ρ.

Jaynes' rule provides a formula for the probabilities in a convex decomposition of ρ in terms of ρ and the elements in the decomposition. In terms of Bloch vectors, it has the form

$$q_k = \frac{1}{2}\frac{1-|\vec{r}|^2}{1-\vec{r}\cdot\hat{s}_k},$$

where we have written $\hat{s}_k$ rather than $\vec{s}_k$ since the elements of the optimal decomposition, being pure, can be represented by unit Bloch vectors. Substituting this expression, together with the constraint that $\vec{r}=q_1\hat{s}_1+q_2\hat{s}_2$ into Eq.(8), we can write P_{Ub} entirely in terms of $\hat{s}_1$,

$$\begin{aligned} P_{Ub} &= \frac{1}{2}\left(1+q_1\left(\hat{a}_1\cdot\hat{s}_1\right)+\left(\hat{a}_2\cdot\vec{r}\right)-q_1\left(\hat{a}_2\cdot\hat{s}_1\right)\right) \\ &= \frac{1}{2}\left(1+\hat{a}_2\cdot\vec{r}\right)+\frac{1}{4}\left(1-|\vec{r}|^2\right)\frac{\left(\left(\hat{a}_1-\hat{a}_2\right)\cdot\hat{s}_1\right)}{\left(1-\vec{r}\cdot\hat{s}_1\right)}. \end{aligned}$$

Rather than varying this quantity with respect to $\hat{s}_1$, we vary with respect to an unnormalized vector $\vec{s}_1$, taking $\hat{s}_1=\vec{s}_1/\left|\vec{s}_1\right|$, where $\left|\vec{s}_1\right|=\sqrt{\vec{s}_1\cdot\vec{s}_1}$. Setting $\delta P_E(\hat{s}_1)=0$ and making use of the fact that $\delta\left|\vec{s}_1\right|=\delta\sqrt{\vec{s}_1\cdot\vec{s}_1}=\delta\vec{s}_1\cdot\hat{s}_1$, we find that the optimal $\hat{s}_1$ satisfies

$$\left(1-\hat{s}_1\cdot\vec{r}\right)\left(\hat{a}_1-\hat{a}_2\right)+\left(\hat{s}_1\cdot\left(\hat{a}_1-\hat{a}_2\right)\right)\left(\vec{r}-\hat{s}_1\right)=0.$$

By assumption, $|\vec{r}|\neq 1$ (since ρ is impure). It follows that $\left(1-\hat{s}_1\cdot\vec{r}\right)\neq 0$, and $\left(\vec{r}-\hat{s}_1\right)\neq\vec{0}$. Since it is also the case that $\left(\hat{a}_1-\hat{a}_2\right)\neq\vec{0}$, we infer that $\hat{s}_1\cdot\left(\hat{a}_1-\hat{a}_2\right)\neq 0$. Taking the dot product of this equation with $\hat{a}_1+\hat{a}_2$, we find

$$\left(\vec{r}-\hat{s}_1\right)\cdot\left(\hat{a}_1+\hat{a}_2\right)=0.$$

Consequently, the solutions that extremize P_{Ub} are of the form

$$\hat{s}_{1\pm}^{\rm ext}=\vec{r}+L_\pm\left(\vec{r}\right)\hat{d},$$

where $\hat{d}$ is given in Eq.(3). The constraint $\left|\hat{s}_{1\pm}^{\rm ext}\right|=1$ implies that $L_\pm\left(\vec{r}\right)$ have the form specified in Eq.(11). Plugging $\hat{s}_{1\pm}^{\rm ext}$ into the expression for P_{Ub}, we find

$$P_{Ub}=\frac{1}{2}\left(1+\hat{a}_1\cdot\vec{r}+L_\pm\left(\vec{r}\right)\left(\hat{a}_1\cdot\hat{d}\right)\right).$$

Since the coefficient of $L_\pm\left(\vec{r}\right)$ is positive, and $L_+\left(\vec{r}\right)\geq L_-\left(\vec{r}\right)$, the maximum P_{Ub} occurs for $\hat{s}_{1+}^{\rm ext}$, while the minimum occurs for $\hat{s}_{1-}^{\rm ext}$. Thus, the optimal $\hat{s}_1$ given $\vec{r}$ is

$$\hat{s}_1^{\rm opt}=\vec{r}+L_+\left(\vec{r}\right)\hat{d}.$$

The constraint $\vec{r}=\sum_k q_k\vec{s}_k$ then implies that

$$\hat{s}_2^{\rm opt}=\vec{r}+L_-\left(\vec{r}\right)\hat{d}.$$

This establishes what we set out to prove.

XI. APPENDIX B

We here present the proofs of the results of section VI.D.1.

Proof for case 1. The parallel condition is equivalent to $\hat{d}_0 = \hat{d}_1$ which implies that $L_{0+} = L_{1+}$, so that Eq.(13) becomes

$$P_U = \frac{1}{2} + \frac{1}{4}\left(\vec{r} + L_{0+}(\vec{r})\,\hat{d}_0\right) \cdot \left(\hat{a}_1^0 + \hat{a}_1^1\right).$$

This is maximized for $\vec{r} + L_{0+}(\vec{r})\,\hat{d}_0 = \frac{\hat{a}_1^0 + \hat{a}_1^1}{|\hat{a}_1^0 + \hat{a}_1^1|}$, which implies that $\vec{r}^{\,\mathrm{opt}}$ can be any vector of the form specified in Eq.(14).□

Proof for case 2. Starting from Eq.(13) , we extremize P_U with respect to variations in $\vec{r}$ by setting $\delta P_U(\vec{r}) = 0$. Using the fact that $\delta r = \delta\sqrt{\vec{r}\cdot\vec{r}} = \delta\vec{r}\cdot\vec{r}/r$, and

$$\delta L_{b+}(\vec{r}) = -\left(\frac{\vec{r} + L_{b+}(\vec{r})\,\hat{d}_b}{\vec{r}\cdot\hat{d}_b + L_{b+}(\vec{r})}\right)\cdot\delta\vec{r},$$

we find that the extremal $\vec{r}$ satisfy

$$\sum_{b=0}^{1}\left(\hat{a}_1^b - \left(\hat{d}_b\cdot\hat{a}_1^b\right)\left(\frac{\vec{r} + L_{b+}(\vec{r})\,\hat{d}_b}{\vec{r}\cdot\hat{d}_b + L_{b+}(\vec{r})}\right)\right) = 0. \qquad (25)$$

We now introduce the notation

$$x_0 = \vec{r}\cdot\hat{d}_1^{\perp}$$
$$x_1 = \vec{r}\cdot\hat{d}_0^{\perp}$$
$$x_2 = \vec{r}\cdot\hat{n},$$

where $\hat{d}_1^{\perp}, \hat{d}_0^{\perp}$ and $\hat{n}$ are defined in Eq. (18). Making use of the fact that $\vec{r} = \left(\vec{r}\cdot\hat{d}_0\right)\hat{d}_0 + \left(\vec{r}\cdot\hat{d}_0^{\perp}\right)\hat{d}_0^{\perp} + (\vec{r}\cdot\hat{n})\,\hat{n}$, we have $\left(\frac{\vec{r}+L_{0+}(\vec{r})\hat{d}_0}{\vec{r}\cdot\hat{d}_0+L_{0+}(\vec{r})}\right) = \hat{d}_0 + \frac{x_1\hat{d}_0^{\perp} + x_2\hat{n}}{\sqrt{1-x_1^2-x_2^2}}$, which together with $\hat{a}_1^0 = \left(\hat{a}_1^0\cdot\hat{d}_0\right)\hat{d}_0 + \left(\hat{a}_1^0\cdot\hat{d}_0^{\perp}\right)\hat{d}_0^{\perp} + \left(\hat{a}_1^0\cdot\hat{n}\right)\hat{n}$ yields

$$\hat{a}_1^0 - \left(\hat{d}_0\cdot\hat{a}_1^0\right)\left(\frac{\vec{r} + L_{0+}(\vec{r})\,\hat{d}_0}{\vec{r}\cdot\hat{d}_0 + L_{0+}(\vec{r})}\right) =$$

$$\left(\hat{a}_1^0\cdot\hat{d}_0^{\perp}\right)\hat{d}_0^{\perp} + \left(\hat{a}_1^0\cdot\hat{n}\right)\hat{n} - \frac{\left(\hat{d}_0\cdot\hat{a}_1^0\right)}{\sqrt{1-x_1^2-x_2^2}}\left(x_1\hat{d}_0^{\perp} + x_2\hat{n}\right).$$

An analogous result holds for $b = 1$. Plugging these expressions into Eq.(25) and taking the dot product with each of $\hat{d}_0, \hat{d}_1$ and $\hat{n}$, we obtain the set of equations

$$0 = \left(\hat{a}_1^1\cdot\hat{d}_1^{\perp}\right)\sqrt{1-x_0^2-x_2^2} - \left(\hat{a}_1^1\cdot\hat{d}_1\right)x_0,$$

$$0 = \left(\hat{a}_1^0\cdot\hat{d}_0^{\perp}\right)\sqrt{1-x_1^2-x_2^2} - \left(\hat{a}_1^0\cdot\hat{d}_0\right)x_1,$$

$$0 = \left(\left(\hat{a}_1^0 + \hat{a}_1^1\right)\cdot\hat{n}\right)\sqrt{1-x_0^2-x_2^2}\sqrt{1-x_1^2-x_2^2}$$
$$- \left(\hat{a}_1^0\cdot\hat{d}_0\right)\sqrt{1-x_0^2-x_2^2}\,x_2 - \left(\hat{a}_1^1\cdot\hat{d}_1\right)\sqrt{1-x_1^2-x_2^2}\,x_2.$$

The values of x_0, x_1 and x_2 that maximize P_U, denoted by $x_0^{\max}, x_1^{\max}$ and $x_2^{\max}$, are easily seen to be those given by Eq.(17). These define $\vec{r}^{\,\max}$ through Eq.(16).

If $|\vec{r}^{\,\max}| \le 1$, then it corresponds to the optimal density operator. If $|\vec{r}^{\,\max}| > 1$, then there is no extremum of P_U inside the Bloch ball and the optimal density operator must be represented by a point on the boundary of the ball. Such a point corresponds to a pure state. Consequently there is no freedom in the convex decomposition Alice realizes, and all that she must decide is what state to tell Bob to test for. If she tells him $|\psi_k^0\rangle$ when she wishes to unveil a bit value of 0 and $|\psi_{k'}^1\rangle$ when she wishes to unveil a bit value of 1, then in terms of Bloch vectors, her probability of unveiling the bit of her choosing is

$$P_U = \frac{1}{4}\left(1 + \hat{r}\cdot\hat{a}_k^0\right) + \frac{1}{4}\left(1 + \hat{r}\cdot\hat{a}_{k'}^1\right)$$
$$= \frac{1}{2} + \frac{1}{4}\hat{r}\cdot\left(\hat{a}_k^0 + \hat{a}_{k'}^1\right),$$

where we write $\hat{r}$ to emphasize that we are varying over pure density operators. The vector $\hat{r} = \frac{\hat{a}_k^0 + \hat{a}_{k'}^1}{|\hat{a}_k^0 + \hat{a}_{k'}^1|}$ clearly maximizes P_U. In our notational convention, $\hat{a}_1^0$ and $\hat{a}_1^1$ are the closest pair of Bloch vectors from the two sets, so Alice should choose $k = k' = 1$. It follows that the optimal density operator is represented by the Bloch vector defined in Eq.(15).

Note that it may occur that $\hat{a}_2^0$ and $\hat{a}_2^1$ are as close to one another as $\hat{a}_1^0$ and $\hat{a}_1^1$, that is, it may occur that there is no unique 'closest' pair of Bloch vectors. However, in this case one will not find $|\vec{r}^{\,\max}| > 1$. The reason is as follows. If one *did* find $|\vec{r}^{\,\max}| > 1$, then the optimal $\vec{r}$ would have to be a pure state. However, since the pure states associated with the Bloch vectors $\frac{\hat{a}_1^0 + \hat{a}_1^1}{|\hat{a}_1^0 + \hat{a}_1^1|}$ and $\frac{\hat{a}_2^0 + \hat{a}_2^1}{|\hat{a}_2^0 + \hat{a}_2^1|}$ would yield the same P_U, any mixture of these would also yield this P_U. This in turn would imply that there existed a solution with $|\vec{r}^{\,\max}| < 1$.□

Proof for case 2.1. Since $\hat{a}_1^0$,$\hat{a}_2^0$, $\hat{a}_1^1$ and $\hat{a}_2^1$ all lie in a plane, $\hat{a}_k^b\cdot\hat{n}$ is independent of b and k. In this case, we find $x_0^{\max} = \hat{a}_1^1\cdot\hat{d}_1^{\perp}$, $x_1^{\max} = \hat{a}_1^0\cdot\hat{d}_0^{\perp}$ and $x_2^{\max} = \hat{a}_1^0\cdot\hat{n}$. That this corresponds to the point of intersection can be verified from the parametric equations for the lines containing the two chords.□

Proof for case 2.2. If the chord defined by $\hat{a}_1^b$ and $\hat{a}_2^b$ passes through the $\hat{n}$ axis, then it must lie in the plane of $\hat{d}_b$ and $\hat{n}$, so that $\hat{a}_k^b\cdot\hat{d}_b^{\perp} = 0$. It follows that $x_0^{\max} = x_1^{\max} = 0$, and thus $\vec{r}^{\,\max} = x_2^{\max}\hat{n}$. Since $|x_2^{\max}| \le 1$, we know that $|\vec{r}^{\,\max}| \le 1$, so that $\vec{r}^{\,\mathrm{opt}} = \vec{r}^{\,\max} = x_2^{\max}\hat{n}$.□

Proof for case 2.3. The case being considered corresponds to $\hat{n}\cdot\left(\hat{a}_k^0 + \hat{a}_k^1\right) = 0$. We must consider the two possibilities $|\vec{r}^{\,\max}| \le 1$ and $|\vec{r}^{\,\max}| > 1$. In the former, $\vec{r}^{\,\mathrm{opt}} = \vec{r}^{\,\max}$, while in the latter $\vec{r}^{\,\mathrm{opt}} = \frac{\hat{a}_1^0 + \hat{a}_1^1}{|(\hat{a}_1^0 + \hat{a}_1^1)|}$. Either way, the condition $\hat{n}\cdot\left(\hat{a}_k^0 + \hat{a}_k^1\right) = 0$ implies that $\vec{r}^{\,\mathrm{opt}}\cdot\hat{n} = 0$.□